SAVING FACE: REGULATING LAW ENFORCEMENT'S USE OF MOBILE FACIAL RECOGNITION TECHNOLOGY & IRIS SCANS

Sabrina A. Lochner*

In 2012, more than 50 law enforcement agencies across the United States began using a mobile device, the Mobile Offender Recognition and Information System ("MORIS"), to identify persons via facial recognition technology ("FRT") and iris scans. No legislative guidelines exist detailing how this personal information can be collected, stored, or used. State and federal case law are silent as to how law enforcement should use MORIS. And although some law enforcement agencies have developed internal guidelines, privacy and policy concerns loom.

This Note explores the privacy and policy concerns raised by MORIS's use and proposes that the Arizona legislature appease these worries. First, the Note details the level of suspicion police officers should obtain before using MORIS by comparing the device to technology that courts have previously considered. Next, the Note discusses policy concerns, such as the possibility for police bias and error. In response, the Note proposes solutions to minimize these concerns. The Note argues that neither law enforcement nor MORIS's developer is positioned to sufficiently mitigate these concerns through self-regulation. In turn, the Note concludes that the state legislature should adopt the Note's recommended guidelines, which strike a balance between MORIS's benefits to law enforcement and citizens' privacy.

---

* J.D. Candidate, University of Arizona James E. Rogers College of Law, 2013. The Author thanks Dean Marc Miller, Shawn Casey, Courtney Henson, Stuart Kottle, Corey Mantei, Victor Nilsson, Steven Schneider, and Julie Wilson-McNerney for their invaluable insight. The Author also extends thanks to her family and Gerard Hugel for their unwavering support.

TABLE OF CONTENTS

INTRODUCTION

Beginning in April 2012, more than 50 law enforcement agencies[1] across the United States began using a mobile device to identify people through facial recognition technology ("FRT"), iris scans, and fingerprints.[2] The device is known as the Mobile Offender Recognition and Information System ("MORIS").[3] Little guidance exists, however, as to how law enforcement agencies, including those in

1. Telephone Interview with Sean Mullin, President & CEO, Biometric Intelligence & Identification Techs. (Mar. 23, 2012).

2. Emily Steel & Julia Angwin, *Device Raises Fear of Facial Profiling*, WALL ST. J., July 13, 2011, at A1.

3. *Id.*

Arizona, should collect, use, and store face and iris data with this portable biometric device. There are currently no reported cases from either state or federal courts regarding law enforcement's use of mobile FRT or iris scans.[4] The Arizona legislature has not regulated how law enforcement should use the device,[5] and the Arizona Constitution's Right to Privacy section merely provides that "[n]o person shall be disturbed in his private affairs, or his home invaded, without authority of law."[6]

While the Federal Constitution's Fourth Amendment provides a baseline level of protection against unreasonable searches and seizures,[7] state legislatures can impose stricter safeguards.[8] As technology advances[9] or comes into general use,[10] the public's reasonable expectation of privacy can diminsh.[11] Thus, states should be wary as to what degree of erosion to permit.

Law enforcement agencies, civil liberty groups, and legal scholars recognize that police might abuse the biometric-based identification device and infringe on the public's privacy rights.[12] Thus, some law enforcement groups have created self-imposed guidelines for when law enforcement officers can take facial pictures and iris scans and run them through the databases.[13] But, these guidelines

---

4. Westlaw searches for "iris scan," "facial recognition technology," and "face scan" in the All Federal & State Cases database yielded no relevant results; *see also* Steel & Angwin, *supra* note 2 (explaining that whether a warrant will be needed for a face or iris scan is a "gray area of the law" (quoting Orin Kerr, Law Professor, George Washington Univ.)).

5. Westlaw search for "biometric" in the Arizona Statutes Annotated database yielded no pertinent results.

6. *See* ARIZ. CONST. art. II, § 8.

7. U.S. CONST. amend. IV.

8. *See* United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring) ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."); *see also* Adam M. Gershowitz, *Texting While Driving Meets the Fourth Amendment: Deterring Both Texting and Warrantless Cell Phone Searches*, 54 ARIZ. L. REV. 577, 620 (2012) (discussing a legislative solution to texting while driving that ensures more privacy protection than the Fourth Amendment for warrantless cell phone searches).

9. *See* Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986) (holding that it is not a search for law enforcement to take aerial photos—from navigable airspace—of an industrial complex).

10. *See* Kyllo v. United States, 533 U.S. 27, 34 (2001).

11. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

12. *See, e.g.*, Zach Howard, *Police to Begin iPhone Iris Scans Amid Privacy Concerns*, REUTERS (July 20, 2011, 2:59 PM), http://www.reuters.com/article/2011/07/20/us-crime-identification-iris-idUSTRE76J4A120110720; Christopher Ott, *Brockton Experiment with Facial Recognition Technology Raises Civil Liberties Concerns*, ACLU MASS. (June 22, 2010, 3:45 PM), http://aclum.org/news_6.22.10; Steel & Angwin, *supra* note 2.

13. *See* Howard, *supra* note 12; Emily Steel, *How a New Police Tool for Face Recognition Works*, WALL ST. J. BLOG (July 13, 2011, 7:56 AM), http://blogs.wsj.com/digits/2011/07/13/how-a-new-police-tool-for-face-recognition-works/; Steel & Angwin, *supra* note 2.

are insufficient;[14] law enforcement lacks accountability to comply, and some policy concerns, such as misuses and biases, remain unaddressed. Developing guidelines for how police should use MORIS remains "a moral responsibility."[15]

This Note urges the Arizona legislature to address when and how law enforcement can collect facial pictures and iris scans; when and how law enforcement can run this data through corresponding databases to ascertain identity and criminal history; and when and how law enforcement can store said data. This Note focuses on Arizona because the Arizona legislature has already expressed sensitivity to regulating the collection of biometric information from students,[16] and the Pinal County Sheriff's Office was one of the first agencies in the country to obtain MORIS.[17]

Part I of this Note describes the development of FRT and iris scans, while Part II details the background of the Fourth Amendment. Part III compares FRT and iris scans to fingerprints, blood and urine samples, voiceprints, and DNA, while analyzing these forensic elements within the context of the Fourth Amendment. Part IV explores whether FRT and iris scans are searches under the Fourth Amendment and thus require reasonable suspicion, probable cause, or consent before collection and use. Part V then details policy concerns, such as potential police bias and error in the collection and use of FRT and iris scans, as motivators for state regulation. The primary policy concerns are (1) the public's lack of notice or ability to opt-out; (2) discriminatory targeting and racial bias; (3) MORIS's possibly unduly suggestive method of operation and unreliable identifications; (4) context bias; (5) function creep; and (6) enrollment of data and database security. Part VI explains why the MORIS developer and police agencies should not be left to self-regulate, and also examines the internal guidelines that some agencies have already adopted. Lastly, in response to the public's privacy and policy concerns, this Note proposes guidelines that the Arizona legislature should adopt regarding law enforcement's collection, use, and storage of facial pictures and iris scans via MORIS. Ultimately, the Note recognizes MORIS's

---

14. While discussing whether it is a Fourth Amendment search for police to attach a GPS device to a vehicle, Justice Sotomayor said that she distrusts the police and believes that they will misuse the technology without "oversight from a coordinate branch." *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).

15. Steel & Angwin, *supra* note 2 (quoting Bill Johnson, Exec. Dir., Nat'l Ass'n of Police Orgs.); *see also* Garrin Groff, *Pinal County Deploying Device That Turns iPhones into I.D. Scanners*, E. VALLEY TRIB. (Oct. 8, 2011, 2:45 PM), http://www.eastvalleytribune.com/local/article_799ba9ae-f13c-11e0-90c1-001cc4c002e0.html ("Law enforcement agencies need clear, written rules on when police can and cannot use the devices and what they do with the information . . . ." (citing Alessandra Soler Meetze, Exec. Dir., ACLU of Ariz.)); Steel, *supra* note 13 (explaining that Bernard Melekian, director of the Office of Community Oriented Policing Services ("COPS") program, thinks there are challenges to creating police guidelines for mobile recognition technology).

16. ARIZ. REV. STAT. ANN. § 15-109 (2013) (requiring schools to obtain written parental or guardian consent before collecting biometric data from a student in a public or charter school); *see also id.* § 1-602(A)(7) (stating that parents have the right to consent in writing before a school does a biometric scan of their minor child).

17. Telephone Interview with Sean Mullin, *supra* note 1.

benefits while insisting that law enforcement obtain accurate results and respect citizens' privacy.

I. DEVELOPMENT OF FACIAL RECOGNITION TECHNOLOGY AND IRIS SCANS

Using FRT, police can determine someone's identity by running a photo of that person's face through a database.[18] The computer program matches the unidentified face with a picture, name, and criminal record of someone already in the database.[19] The program works by calculating the distances between facial features, such as one's eyes.[20] Next, it uses an algorithm to see if any pictures in the database match the facial measurements in the provided photo.[21] Police thus use FRT to identify people who are not carrying identification cards or those who are carrying false identification.[22] FRT also helps police learn the identity of persons from afar to see if warrants are out for their arrest or if they are on watch lists.[23]

A serious concern arises, however, because police have not always warned the public when they are using FRT.[24] For example, unbeknownst to Super Bowl XXXV attendees in 2001, police ran the spectators' facial images through a database as they entered the stadium.[25] The American Civil Liberties Union ("ACLU") expressed outrage upon learning about this covert surveillance and claimed that it may have violated the Fourth Amendment.[26]

Despite the lack of notice as to when law enforcement would use this technology, police were initially limited to using FRT in a stationary manner during the technology's infancy.[27] In addition to the 2001 Super Bowl, law enforcement agencies also employed stationary FRT on city streets and in airports.[28] That same year, the Tampa Police Department installed FRT cameras in

---

18. Howard, *supra* note 12.

19. *See* Steel, *supra* note 13.

20. *Q&A on Face Recognition*, ACLU (Sept. 2, 2003), http://www.aclu.org/technology-and-liberty/qa-face-recognition.

21. *See* Peter Murray, *Police Across U.S. to Use Face Scanners to ID Suspects*, SINGULARITY HUB (July 25, 2011, 1:39 AM), http://singularityhub.com/2011/07/25/police-across-the-us-to-use-face-scanners-to-id-suspects/.

22. Steel & Angwin, *supra* note 2.

23. *See* Declan McCullagh, *Call It Super Bowl Face Scan I*, WIRED (Feb. 2, 2001), http://www.wired.com/politics/law/news/2001/02/41571.

24. *Id.*

25. McCullagh, *supra* note 23; *Q&A on Face Recognition*, *supra* note 20.

26. McCullagh, *supra* note 23.

27. *See* Joyce W. Luk, Note, *Identifying Terrorists: Privacy Rights in the United States and the United Kingdom*, 25 HASTINGS INT'L & COMP. L. REV. 223, 223, 226–27 (2002).

28. *See* Brady Dennis, *Ybor Cameras Won't Seek What They Never Found*, ST. PETERSBURG TIMES, Aug. 20, 2003, at 1A; Thomas Frank, *Face-Recognition Systems Weighed as Next Weapon Against Terrorism*, USA TODAY, May 10, 2007, at 01A.

the nightlife area of Ybor City, Florida,[29] and the Virginia Department of Criminal Justice Services funded FRT cameras in Virginia Beach to find criminal suspects and missing children.[30] In 2002, Boston's Logan Airport tested FRT as an additional security measure after 9/11.[31] But the technology proved to be unreliable in these early years. Logan Airport's system failed to positively identify volunteers pretending to be terrorists 39% of the time[32] and consequently the airport abandoned FRT.[33] Similarly, Tampa and Virginia Beach removed the cameras after their use failed to result in arrests.[34]

As the technology has advanced, however, FRT has become more reliable and mobile. For example, the American military began using a multi-modal device called Handheld Interagency Identity Detection Equipment ("HIIDE") in 2007.[35] This allowed soldiers to take facial pictures, iris scans, and fingerprints in the field and compare the gathered information to a database; the comparison let soldiers see if the person being scanned was on a watch list and allowed the soldiers to determine the person's identity.[36] If the person did not appear on a watch list, the soldier could save that person's information.[37] By the end of 2009, soldiers in Iraq and Afghanistan were using more than 7,000 HIIDE devices to distinguish insurgents from civilians and to enroll them into the database.[38] Despite Afghans' concerns that the biometric database—operated by the United States, NATO, and local groups—could be used against them as an ethnic, tribal, or political weapon, the American military continued to collect biometric information from Afghans and Iraqis in 2011.[39]

Iris scans, as used in HIIDE devices, work similarly to FRT. Iris scans confirm the identity of someone by detecting the unique color pattern of an individual's eye and mathematically finding a match previously entered into a database.[40] In 2007, *USA Today* reported that iris scans could detect 235 unique

---

29. Dennis, *supra* note 28.

30. *Face Recognition*, EPIC, http://epic.org/privacy/facerecognition/ (last visited Mar. 1, 2013).

31. Stephanie Ebbert, *New Tool for Police Is Good with Faces*, BOS. GLOBE, July 18, 2011, at B1.

32. Frank, *supra* note 28.

33. Ebbert, *supra* note 31.

34. Frank, *supra* note 28.

35. Jody Kieffer & Kevin Trissell, *DOD Biometrics—Lifting the Veil of Insurgent Identity*, ARMY AL&T, April–June 2010, at 14, 16.

36. *Id.*

37. *Id.*

38. *Id.* at 17.

39. Thom Shanker, *To Track Militants, U.S. Has System That Never Forgets a Face*, N.Y. TIMES, July 13, 2011, at A1. HIIDE helped locate some of the 475 insurgents who escaped from Sarposa Prison in Afghanistan. *Id.*

40. Howard, *supra* note 12.

identifiers without skewing results from Lasik surgery or disease; fingerprinting only detects about 70 details.[41]

Law enforcement used iris scans in prisons as early as 1996 to ensure release of the correct inmate.[42] In 2002, John F. Kennedy International Airport became the first American airport to install iris-scanning technology for use by employees.[43] From 2004 to 2008, the Transportation Security Administration offered a paid, opt-in Registered Traveler program, where passengers could provide either fingerprints or an iris scan to use as their identification when flying.[44] About 20 airports participated in the program, which was operated by private companies.[45] However, the program ended when the TSA found it did not trust the machines' reliability.[46] In 2007, more law enforcement agencies began using iris scans on sex offenders, runaways, abducted children, and Alzheimer's patients.[47] The cost of iris scan systems, however, has presented an obstacle to law enforcement groups.[48]

Although the military has used portable multi-modal biometric devices to make identifications for several years, law enforcement did not test MORIS until 2010.[49] MORIS attaches to an iPhone and allows law enforcement officers to search facial, iris, and fingerprint databases while they are in the field.[50] This helps officers ascertain the identity and criminal history of the person whose biometric

---

41. Wendy Koch, *Iris Scans Let Law Enforcement Keep an Eye on Criminals*, USA TODAY, Dec. 5, 2007, at A1.

42. Associated Press, *Jails Hope Eye Scanners Can Provide Foolproof Identification System for Inmates*, N.Y. TIMES, Feb. 27, 2007, at A25.

43. Associated Pres, *JFK Airport Begins Iris Scans*, L.A. TIMES (Nov. 15, 2002), http://articles.latimes.com/2002/nov/15/nation/na-scan15.

44. Benet Wilson, *Could We Be Closer to a Trusted Traveler Program?*, AVIATION WK (Mar. 18, 2011, 5:12 PM), http://www.aviationweek.com/Blogs.aspx?plckBlogId=Blog%3a7a78f54e-b3dd-4fa6-ae6edff2ffd7bdbb&plckPostId=Blog%3a7a78f54e-b3dd-4fa6-ae6e-dff2ffd7bdbbPost%3a0f223001-1f90-4e89-ab1b-bb803d1967ec.

45. *Id.*

46. *Id.*

47. Koch, *supra* note 41.

48. Associated Press, *supra* note 42 (explaining that iris scans have generally been around for at least a decade, but the average law enforcement agency cannot afford the technology). The technology remains expensive as each MORIS device costs $3,000; this price includes the iPhone. Steel, *supra* note 13.

49. Steel & Angwin, *supra* note 2; Edecio Martinez, *iPhone Technology Future Crime Fighters' Best Friend? Matches Eyes, Facial Features to Data Base*, CBSNEWS (June 16, 2010, 7:05 AM), http://www.cbsnews.com/8301-504083_162-20007790-504083.html. The Plymouth County Sheriff's Department and the Brockton Police Department, both in Massachusetts, were the two agencies that tested MORIS in 2010. *See BI2 Technologies of Plymouth, Mass. Begins Implementation of MORIS—a First-of-its-Kind iPhone-Based Mobile and Wireless Multi-Modal Biometric Offender Recognition and Information System—in Conjunction with Statewide Facial Recognition Project*, BUS. WIRE (June 14, 2010, 7:52 AM), http://www.businesswire.com/news/home/20100614005948/en/BI2-Technologies-Plymouth-Mass.-Begins-Implementation-MORIS%E2%84%A2.

50. Steel & Angwin, *supra* note 2.

information they run through the database.[51] Police can take a picture of the subject's face from up to 5 feet away and conduct an iris scan from up to 6 inches from the person's eye.[52] The device matches photographs against a national criminal records database that is managed by Biometric Intelligence and Identification Technologies ("BI2 Technologies"), the private company that designed MORIS.[53] The database consists of criminal records and face images collected by local law enforcement agencies using BI2 Technologies' products.[54] Some states have added mug shots, but the database mainly consists of people who have been either admitted to or released from correctional facilities.[55] If there is an algorithmically based facial match, MORIS will return a set of comparable photos.[56] The officer then selects the correct photo from those the program has flagged as similar.[57] Likewise, the iris scans are matched against an iris database shared among participating agencies.[58]

More than 50 law enforcement agencies were slated to start using MORIS beginning in April 2012.[59] The Supreme Court has not declared whether using FRT and iris scans are Fourth Amendment searches; this has forced law enforcement to navigate the device's constitutionality without judicial guidance.[60] Nevertheless, the Court has previously analyzed police collection of other identifying information, which provides some insight into how and when law enforcement may permissibly collect face and iris scans.[61] However, relying solely on the Fourth Amendment does little to protect anonymity[62] or prevent police discretion and biases from interfering with accurate identifications.[63] Because

---

51. Steel, *supra* note 13.

52. Steel & Angwin, *supra* note 2.

53. Murray, *supra* note 21.

54. Steel & Angwin, *surpa* note 2. The FBI plans to eventually make its face data available for MORIS searching too. Telephone Interview with Sean Mullin, *supra* note 1.

55. Steel & Angwin, *surpa* note 2.

56. BI2Technologies, *MORIS Handheld Iris/Face/Fingerprint Biometric Recognition Device*, YOUTUBE (June 14, 2010), http://www.youtube.com/watch?v=jk-NL71IwjY.

57. *Id.*

58. Lindsey Collom, *Pinal Sheriff's Office Sees Eye Scanners as Future*, ARIZ. REPUB. (May 6, 2011, 12:00 AM), http://www.azcentral.com/arizonarepublic/local/articles/2011/05/06/20110506pinal-sheriff-eye-scanners-identification.html#ixzz1RmLg7CWa.

59. Telephone Interview with Sean Mullin, *supra* note 1.

60. *See* D. Parvaz, *Mobile Biometrics to Hit U.S. Streets*, ALJAZEERA (Aug. 2, 2011, 4:25 PM), http://english.aljazeera.net/indepth/features/2011/07/20117258145965608.html ("I'm dancing on the head of a pin here because I'm not a constitutional scholar." (quoting John Birtwell, Dir. of Pub. Info. & Tech., Plymouth Cnty. Sheriff's Dep't)).

61. *See* United States v. Diaz-Castaneda, 494 F.3d 1146, 1152 (9th Cir. 2009); *infra* Part III.

62. *See infra* Part IV.

63. *See Diaz-Castaneda*, 494 F.3d at 1152 (discussing why potential police error while running license plate numbers through a database lacks Fourth Amendment protection). "[T]he possibilities of database error and police officer abuse, while real, do not create a legitimate expectation of privacy where none existed before. Government actions

MORIS identifications may be imperfect, the Arizona legislature should provide oversight. Some law enforcement agencies have created self-imposed restrictions on when to collect and analyze facial images and iris scans, but this does not quell concerns about privacy violations, especially with regard to the enrollment of facial or iris images.[64] With no accountability to anyone but themselves, law enforcement groups may stray from their guidelines. Affirmative state legislation would make law enforcement agencies accountable while ensuring privacy where the Fourth Amendment may not.[65]

II. FOURTH AMENDMENT BACKGROUND

The Fourth Amendment of the U.S. Constitution protects people from unreasonable searches and seizures and requires probable cause before a judge can issue a warrant.[66] The warrant must detail the place to be searched and the things to be seized.[67] "The overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State."[68] To determine if something is a search and deserves Fourth Amendment protection, courts employ the reasonable expectation of privacy test from the concurrence in *United States v. Katz* and the trespass test from *United States v. Jones*.[69]

If a person exhibits a subjective expectation of privacy and society sees that expectation as reasonable, then police interference with that expectation is a search.[70] If there is no subjective and objective expectation of privacy, then Fourth Amendment protections do not apply; it is not a search for the police to obtain that information.[71] "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[72] To determine whether someone has a reasonable expectation of privacy, the Supreme Court has held that if a person exposes something to a third-party, he assumes the risk that it will be exposed to law enforcement.[73] For example, in *United States v. White*, a person assumed the risk and had no reasonable expectation of privacy to

---

do not become Fourth Amendment searches simply because they *might* be carried out improperly." *Id.*

64. *See* Steel, *supra* note 13.

65. Congress enacted regulation regarding wiretapping to protect the public from intrusions of privacy instead of relying on the courts to analyze the applicable Fourth Amendment case law. United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring).

66. U.S. CONST. amend. IV.

67. *Id.*

68. Schmerber v. California, 384 U.S. 757, 767 (1966).

69. *Jones*, 132 S. Ct. at 953–54; United States v. Katz, 389 U.S. 347, 360–63 (1967) (Harlan, J., concurring).

70. *Katz*, 389 U.S. at 361 (Harlan, J., concurring); *see Jones*, 132 S. Ct. at 954–55.

71. *See Katz*, 389 U.S. at 361 (Harlan, J., concurring).

72. *Id.* at 351 (Stewart, J., majority).

73. United States v. White, 401 U.S. 745, 752 (1971).

incriminating information he revealed to an informant, who was transmitting the conversation to police.[74]

Generally, it is not a search for police to obtain publicly exposed evidence while enhancing their senses with technology.[75] For instance, it is not a search for police to fly over a manufacturing facility and take aerial pictures.[76] But the Supreme Court has acknowledged that law enforcement's use of some sense-enhancing technology may constitute a search.[77] In *Dow Chemical Co. v. United States*, the Court noted that some "sophisticated surveillance equipment not generally available to the public, such as satellite technology," may require a warrant.[78] The Court also hinted that photographs revealing intimate details may be searches; after all, the Court emphasized that aerial photos were not a search in part because they were "not so revealing of intimate details as to raise constitutional concerns."[79] Additionally, in *Kyllo v. United States*, the Court determined that it was a search to use technology not in general use to get information from inside a house that could not "otherwise have been obtained without a physical intrusion."[80] Law enforcement had used a thermal imager to scan a house and see heat, consistent with a marijuana grow room, emanating from the attic.[81] Although *Kyllo* dealt with extracting information from inside a home—a place usually seen as highly protected by an expectation of privacy—the Court also noted that the public generally did not use thermal imagers and so found its use analogous to a search.[82]

More recently, the Supreme Court held in *United States v. Jones* that when police attached a Global Positioning System ("GPS") device on someone's car and tracked the vehicle on public streets for 28 days, this constituted a Fourth Amendment search.[83] The majority utilized a trespass test—that exists concurrently with the *Katz* test—and found that placing a GPS device on a car to track a person's whereabouts was a search.[84] The Court said it should apply "an 18th-century guarantee against unreasonable searches, which we believe must provide *at a minimum* the degree of protection [the Fourth Amendment] afforded when it was adopted."[85] The Court affirmed that visual observation is not a search; however, the Court did not answer whether electronic surveillance that is not a

---

74. *Id.* at 751.

75. *See generally* Dow Chem. Co. v. United States, 476 U.S. 227, 238–39 (1986).

76. *Id.* at 239.

77. *See* United States v. Jones, 132 S. Ct. 945, 947–49 (2012); Kyllo v. United States, 533 U.S. 27, 29–30, 40 (2001); *Dow Chem. Co.*, 476 U.S. at 239.

78. 476 U.S. at 238.

79. *Id.* (describing the aerial photographs as limited to showing the outlines of buildings and equipment).

80. 533 U.S. at 40, 46.

81. *Id.* at 29–30.

82. *Id.* at 40.

83. 132 S. Ct. 945, 949 (2012).

84. *Id.* at 949, 953.

85. *Id.* at 953.

trespass, but that lasts for an extended period of time, could be a search.[86] Viewing the majority and concurring opinions together, scholars think the Court may be ready to adopt a "mosaic theory" of the Fourth Amendment.[87]

The mosaic theory approach would evaluate the sum of law enforcement actions over a period of time to determine if a reasonable expectation of privacy exists.[88] Police using GPS for a day to track someone may not be a search, but if police use GPS surveillance for a month, the non-search may become a Fourth Amendment search.[89] As the government combines individual parcels of information, the collective information may gain greater meaning and become more intrusive.[90] Essentially, the mosaic theory would require courts to look at the "collective sequence of government activity as an aggregated whole to consider whether the sequence amounts to a search."[91]

Currently, under the plain view doctrine, an officer can, without a warrant, seize an item whose incriminating character is immediately apparent from a lawful vantage point.[92] "A truly cursory inspection—one that involves merely looking at what is already exposed to view, without disturbing it—is not a 'search' for Fourth Amendment purposes, and therefore does not even require reasonable suspicion."[93]

If police have reasonable suspicion that a person has committed, is committing, or is about to commit either a violent or nonviolent crime, they may stop the person in order to investigate further.[94] The intrusion on the person's privacy is balanced with the officers' safety.[95] As the subject of one of these *Terry* stops, a person does not have an absolute right to be anonymous to police.[96] Knowing someone's identity and his past criminal conduct helps officers assess their safety.[97] If a state has a stop-and-identify statute, and police inform a man

---

86. *Id.* at 953–54.

87. *See, e.g.*, Orin Kerr, *What's the Status of the Mosaic Theory After* Jones?, VOLOKH CONSPIRACY (Jan. 23, 2012, 1:59 PM), http://volokh.com/2012/01/23/whats-the-status-of-the-mosaic-theory-after-jones/.

88. *Id.*

89. Orin Kerr, *D.C. Circuit Introduces "Mosaic Theory" of Fourth Amendment, Holds GPS Monitoring a Fourth Amendment Search*, VOLOKH CONSPIRACY, (Aug. 6, 2010, 2:46 PM), http://www.volokh.com/2010/08/06/d-c-circuit-introduces-mosaic-theory-of-fourth-amendment-holds-gps-monitoring-a-fourth-amendment-search/.

90. Madelaine Virginia Ford, Comment, *Mosaic Theory and the Fourth Amendment: How* Jones *Can Save Privacy in the Face of Evolving Technology*, 19 AM. U. J. GENDER SOC. POL'Y & L. 1351, 1363–64 (2012) ("The fear of the unknown value of collective information should also protect an individual's fundamental right to privacy from highly intrusive government searches.").

91. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 311 (2012).

92. Arizona v. Hicks, 480 U.S. 321, 326 (1987).

93. *Id.* at 322.

94. *See* Terry v. Ohio, 392 U.S. 1, 29–31 (1968).

95. *Id.* at 26.

96. Hiibel v. Sixth Jud. Dist. Ct. of Nev., 542 U.S. 177, 185–87 (2004).

97. *Id.* at 186.

that it is unlawful not to identify himself, officers can arrest the man if he fails to provide identification.[98] In Arizona, a person must give his full name upon an officer's request; however, no additional answers need be given.[99]

Understanding how the Court has interpreted the Federal Constitution's Fourth Amendment with regard to classifying searches informs this Note's analysis of whether FRT or the iris scan capability in MORIS should be deemed a search. If MORIS's capabilities are searches under the Fourth Amendment, it would be unlawful for police to take facial pictures or iris scans and run them through the corresponding databases on anything less than consent or probable cause and a warrant. If using FRT or running iris scans are more similar to mere visual observation from a lawful vantage point, then consent or police suspicion of a person's wrongdoing need not be obtained. If consent or any level of suspicion is not required under the Fourth Amendment, then the state may nonetheless limit when police can use MORIS. Arizona's stop-and-identify statute shows when police can ascertain one's identity and may help establish a framework for when it is appropriate for police to demand knowledge of a person's identity via MORIS. This framework could inform state regulation. Given that the Court has not explicitly analyzed mobile FRT or iris scans, this Note next explores whether the collection of other biometric information constitutes searches under the Fourth Amendment and what level of suspicion police must garner before collection.

III. HOW THE SUPREME COURT HAS APPLIED THE FOURTH AMENDMENT TO OTHER TECHNOLOGIES THAT COLLECT BIOMETRIC INFORMATION

A. Fingerprints

For law enforcement to take fingerprints in the field, the Court has suggested that the officer must have at least reasonable suspicion that the person to be fingerprinted has committed a crime or is committing a crime.[100] Also, the officer may only take the fingerprints if they will reasonably show whether the person was connected to the crime.[101] Fingerprinting does not probe "into the private life and thoughts" of a person, so it "represents a much less serious intrusion upon personal security than other types of searches and detentions."[102] However, under the Fourth Amendment, the Court has held that probable cause is necessary to detain an individual, force him to travel to the police station, and make him submit to fingerprinting.[103] But the Arizona Court of Appeals has

98. *Id.* at 186–90.
99. ARIZ. REV. STAT. ANN. § 13-2412 (2013).
100. Hayes v. Florida, 470 U.S. 811, 817 (1985).
101. *Id.*
102. *Id.* at 814 (citing Davis v. Mississippi, 394 U.S. 721, 727 (1969)).
103. *Id.* at 816.

concluded that police should not collect fingerprints from an undetained person, such as a victim, on anything less than individualized reasonable suspicion.[104]

> The gathering of fingerprint evidence from 'free persons' [as contrasted with those in custody] constitutes a sufficiently significant interference with individual expectations of privacy that law enforcement officials are required to demonstrate that they have probable cause, or at least an articulable suspicion, to believe that the person committed a criminal offense and that the fingerprinting will establish or negate the person's connection to the offense.[105]

B. Voiceprints

Unlike bodily intrusions, such as collecting blood, the Supreme Court has held that obtaining bodily information from someone that the public consistently sees or hears does not constitute a search under the Fourth Amendment.[106] For example, "[l]ike a man's facial characteristics, or handwriting, his voice is repeatedly produced for others to hear. No person can have a reasonable expectation that others will not know the sound of his voice, any more than he can reasonably expect his face will be a mystery to the world."[107]

C. Blood, Urine, and DNA Samples

It is a Fourth Amendment search for police to collect a person's blood or urine, because these are not usually exposed to the public and people have a reasonable expectation of privacy in them.[108] But under certain conditions and in certain jurisdictions, police may reasonably collect blood without a warrant.[109] For instance, in *Schmerber v. California*, the Court held that it was reasonable under the Fourth Amendment for police to withdraw blood involuntarily and without a warrant when they had probable cause that someone had been driving while intoxicated and police had arrested the person.[110] The Court justified the bodily intrusion by reasoning that the police needed to gather evidence before the alcohol in the blood dissipated.[111] The Court weighed how a blood test affected the suspect's health, the extent to which it would intrude on the person's personal privacy and bodily integrity, and the state's law enforcement interest.[112] In Arizona, however, a heightened standard exists; police can ask a person arrested

---

104. Romley v. Schneider, 45 P.3d 685, 688 (Ariz. Ct. App. 2002) (citing Rise v. Oregon, 59 F.3d 1556, 1559 (9th Cir. 1995)).
105. *Id.*
106. United States v. Dionisio, 410 U.S. 1, 14–15 (1973).
107. *Id.*
108. Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 617 (1989).
109. Schmerber v. California, 384 U.S. 757, 770–72 (1966).
110. *Id.*
111. *Id.*
112. *Id.*

for driving under the influence to submit to a blood test, but police generally may not administer the test absent a warrant, unless the subject has given consent.[113]

Urine samples also intrude on reasonable expectations of privacy, so they are Fourth Amendment searches.[114] But, urine samples can be reasonably collected without a warrant so that law enforcement can perform a "special needs" function that goes beyond simple law enforcement, such as ensuring that employees in safety-sensitive jobs are not intoxicated.[115]

Taking and analyzing DNA or saliva is also a Fourth Amendment search, but it can be reasonably done without a warrant where there is minimal intrusion and a legitimate government interest.[116] The Supreme Court has not heard a DNA collection case, but the "U.S. Courts of Appeals for the First, Second, Sixth, Seventh, Eighth, Ninth, Tenth, and Eleventh Circuits [each] upheld the 2004 version of the federal DNA collection law, which authorized collection and analysis of DNA from people convicted of any felony, certain sexual crimes, and crimes of violence."[117] Federal courts of appeals have also upheld state DNA-collection laws.[118] The rationale for these rulings is that collecting DNA from inmates to create a law enforcement database is justified in part because inmates have diminished privacy protection.[119]

IV. APPLYING THE FOURTH AMENDMENT ANALYSIS TO MORIS AND RECOGNIZING PRIVACY CONCERNS

A. Mobile Facial Recognition Technology

Applying the *Katz* reasonable expectation of privacy test to FRT, a court will likely find that it is not a search for an officer to take a picture of someone's face and run it through a database to find a match. Given that a person exposes his face to the public daily, privacy of facial characteristics is not a right the public will likely recognize as reasonable.[120] Just as it is not a search for police to take aerial photographs of a manufacturing plant,[121] it cannot be a search to take pictures of people's faces in public places.

---

113. Carrillo v. Houser, 232 P.3d 1245, 1245 (Ariz. 2010) (en banc).

114. Petersen v. City of Mesa, 83 P.3d 35, 38 (Ariz. 2004) (en banc) (citing Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 617 (1989)).

115. Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 619–24 (1989) (holding that despite not having a warrant or individualized suspicion, the Government could test railroad employees to see if they had drugs or alcohol in their bodies).

116. 68 AM. JUR. 2D *Searches and Seizures* § 98 (2013).

117. ANNA C. HENNING, CONG. RESEARCH SERV., R40077, COMPULSORY DNA COLLECTION: A FOURTH AMENDMENT ANALYSIS 7-5700, at 9–10 (2010), *available at* http://www.fas.org/sgp/crs/misc/R40077.pdf.

118. *Id.* at 10.

119. Boling v. Romer, 101 F.3d 1336, 1339–40 (10th Cir. 1996). Persons on probation also have diminished privacy expectations. United States v. Knights, 534 U.S. 112, 119–20 (2001).

120. *See* United States v. Dionisio, 410 U.S. 1, 14 (1973).

121. Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986).

Arguably MORIS's FRT is a search because mobile FRT is not in general use and the photos reveal intimate details not visible without sensory-enhancing technology. But this argument would likely fail because FRT reveals facial details, which are less intimate than aerial photos that can reveal an industry's trade secrets.[122] Additionally, the Court in *Kyllo* relied on a thermal imager's intrusion into the home to find that the *use* of the technology constituted a search seemingly more than the technology's *novelty*.[123] Although the Supreme Court has indicated that it will tend to treat items not widely used by the public as searches, the Court gives this consideration little weight. After all, in *Dow Chemical Co.* it was a non-search for police to be taking pictures with a $22,000 aerial camera.[124] Thus, there is little traction for the argument that using MORIS is a search because it is not in general use.

Interestingly, FRT takes the photograph a step further and runs it through a database to see if there is a facial match. Most circuit courts have shown that it is lawful to run legally obtained information through a database.[125] In *United States v. Ellison*, the Sixth Circuit held that police running a license plate number through a database did not trigger the Fourth Amendment.[126] There was no reasonable expectation of privacy in the license plate number, which the police observed from a lawful vantage point.[127] Thus, some law enforcement agencies have begun using an Automated License Plate Recognition program, which attaches a camera on top of a police car and runs every license plate it detects through an FBI hotlist to ascertain information, such as whether the car is stolen.[128] These agencies have used picture-taking and database-running technologies without probable cause or even reasonable suspicion regarding a particular car.[129] Similarly, if law enforcement were to use MORIS from a lawful vantage point, Fourth Amendment protections probably would not be implicated; neither probable cause nor reasonable suspicion would be required to collect facial pictures and to run searches.

Although FRT is a biometric form of identification, it is distinguishable from fingerprints, bodily fluids, and DNA. First, fingerprints, bodily fluids, and DNA are not as obviously exposed to the public, so there is a heightened expectation of privacy. Second, bodily contact with the suspect is generally required to acquire these identifications, unlike a photograph. Third, DNA can

---

122. *See id.* at 232, 238.

123. Kyllo v. United States, 533 U.S. 27, 35–41 (2001).

124. 476 U.S. at 242–43, n. 4.

125. *See* United States v. Diaz-Castaneda, 494 F.3d 1146, 1150 (9th Cir. 2009) (stating that every circuit court that has decided the issue has held that license plate checks are not searches).

126. 462 F.3d 557, 561–63 (6th Cir. 2006).

127. *Id.*

128. Peter Murray, *Big Brother Can Drive—Police Car-Mounted Cameras Scan 10,000 License Plates Per Hour*, SINGULARITY HUB (May 4, 2011, 8:15 AM), http://singularityhub.com/2011/05/04/big-brother-can-drive-police-car-mounted-cameras-scan-10000-license-plate-per-hour/; *see also* Murray, *supra* note 21.

129. *See* Murray, *supra* note 128.

reveal one's "diseases, traits, and predispositions" in addition to information about those in the person's bloodline.[130] Looking to the identification measures discussed in Part III as a guide, FRT probably is not a search that requires probable cause, reasonable suspicion, or consent.

At first glance, *Jones* seems to lay the groundwork for classifying FRT as a Fourth Amendment search: FRT may not give people the minimum degree of protection the Fourth Amendment originally intended.[131] But this interpretation is flawed. First, the majority emphasizes "that mere visual observation does not constitute a search."[132] Second, *Jones* finds it determinative that the police placed a physical device on someone's car and "occupied private property for the purpose of obtaining information."[133] Conversely, FRT does not require a physical trespass and taking and analyzing these pictures could be categorized as "mere visual observation."[134] Thus, under both the trespass test and *Katz* test, FRT is not likely to be a Fourth Amendment search.

Perhaps the Court would be more willing to classify FRT as a search under the mosaic theory that five Justices in *Jones* seemed ready to adopt.[135] If police use FRT pervasively and without even reasonable suspicion, this presents a question similar to that left open in *Jones*: whether to treat prolonged electronic surveillance without an accompanying trespass as a search.[136] Although the mosaic theory seems like the most viable avenue for classifying certain FRT use as a Fourth Amendment search, the Supreme Court has yet to authenticate the test.[137] Hence, legislators are probably best equipped to protect the public's privacy from the police's use of sense-enhancing technology.[138]

---

130. *Genetic Privacy*, EPIC, http://epic.org/privacy/genetic/ (last visited Mar. 1, 2013).

131. *See* United States v. Jones, 132 S. Ct. 945, 953 (2012).

132. *Id.*

133. *Id.* at 949.

134. This analysis assumes that the pictures were taken from a lawful vantage point.

135. *See* Kerr, *supra* note 87.

136. *Jones*, 132 S. Ct. at 954 (noting that if police use electronics from afar to track someone's whereabouts for up to four weeks, this may be an unconstitutional privacy invasion). If the public is continuously monitored by FRT or if an individual's whereabouts can be tracked for an extended period of time via FRT, then the concerns presented, but unanswered, in *Jones* resurface.

137. *See* Kerr, *supra* note 91, at 330–32 (discussing three different mosaic theory approaches offered by the Justices).

138. *See* David E. Steinberg, *Sense-Enhanced Searches and the Irrelevance of the Fourth Amendment*, 16 WM. & MARY BILL RTS. J., 465, 467 (2007) ("Given the inapplicability of the Fourth Amendment, the regulation of powerful new search techniques should come from statutes written by elected legislators.").

B. Mobile Iris Scans

Currently, iris scans share many similarities with fingerprinting.[139] Although individuals technically expose their fingers and eyes to the public, a closer inspection is required to make sense of the identifying information each contains. For fingerprints, this means briefly detaining someone to make them submit to fingerprint collection. Likewise, MORIS currently requires iris scans to be taken 6 inches from the eye, thus requiring the subject's cooperation.[140] Since fingerprints' identifying elements are not easily observed and irises can reveal health information,[141] this may implicate a reasonable expectation of privacy and require that the police officer have at least reasonable suspicion.[142]

As technology advances, however, police will be able to take iris scans from farther distances without detaining someone.[143] This may diminish the public's reasonable expectation of privacy. The *Katz* test lets technology lessen reasonable expectations of privacy as gadgets become more common and less intrusive.[144] Under this test, iris scans may not be searches. Using its rationale in *Jones*, the Court could find that iris scans violate the Fourth Amendment's minimum protection and constitute searches; however, the Court found the physical trespass in *Jones* important, and iris scans have no element of physical trespassing. Under the mosaic theory suggested in *Jones*, though not adopted by the Court,[145] it is possible that iris scans may be considered searches if law enforcement begins to employ them in a pervasive manner or combines iris scan information with other data. If iris scans are not Fourth Amendment searches, police can obtain scans without a warrant, probable cause, or reasonable suspicion.

---

139. Parvaz, *supra* note 60 ("An iris scan is almost certainly 'a search' within the meaning of the Fourth Amendment's protection against unreasonable searches and seizures. The closest analogy is of course a fingerprint." (quoting Laurence Tribe, Constitutional Law Professor, Harvard Law Sch.)).

140. Steel & Angwin, *supra* note 2. If a subject chooses to keep his eyes closed, then a warrant might be needed to force the subject to open his eyes and submit to an iris scan, says Orin Kerr, law professor at George Washington University. *Id.*

141. *See* Eur. Parl. Ass., *The Need for Global Consideration of the Human Rights Implications of Biometrics*, Mar. Standing Comm., Doc. No. 12522, at 9 (2011), *available at* http://assembly.coe.int/ASP/Doc/XrefViewPDF.asp?FileID=13103&Language=EN.

142. Romley v. Schneider, 45 P.3d 685, 688 (Ariz. Ct. App. 2002) (citing Rise v. Oregon, 59 F.3d 1556, 1559 (9th Cir. 1995)). *Dow Chemical Co.* suggested that when police take warrantless photographs that reveal intimate details, this may raise Fourth Amendment concerns. Dow Chem. Co. v. United States, 476 U.S. 227, 238 (1986).

143. Jim Garrettson, *Multimodality: The Brave New World of Biometrics*, EXECUTIVEGOV (Nov. 16, 2010), http://www.executivegov.com/2010/11/multimodality-the-brave-new-world-of-biometrics/ ("[S]ome companies are developing iris scans that would identify subjects from a distance of as much as 10 meters.").

144. *Kyllo* noted that technology not used by the general public is more analogous to a search, whereas technology used by the public generally is less likely to be a search. Kyllo v. United States, 533 U.S. 27, 40 (2001).

145. *See* Kerr, *supra* note 87. Although the Court seemed open to adopting the mosaic theory, it stated that "the present case does not require us to answer that question." United States v. Jones, 132 S. Ct. 945, 953 (2012).

Legislation about how law enforcement can gather and use iris data would give the public an *ex ante* privacy protection from iris scans instead of waiting for courts to interpret the Fourth Amendment's application to iris scans.

V. POLICY CONCERNS WEIGH IN FAVOR OF STATE LEGISLATIVE REGULATION OF MORIS

The mobility of MORIS makes it impracticable for citizens to avoid police using the technology; there is no opt-out option. And MORIS's design leaves room for police bias and error in its operation. These biases manifest themselves in the form of discriminatory targeting, racial bias, and context bias. This means that police may more frequently use MORIS to identify certain groups of people without oversight; police may not be able to correctly identify the facial features of a person of another race to make accurate identifications; and outside distractions may cause the police to make incorrect identifications. The technology also does not eliminate errors inherent in lineups or the possibility of the data being collected and stored for unanticipated purposes. Lastly, the facial and iris databases are unregulated and have no guidelines for how to enroll new persons. This Part addresses each of these policy concerns and proposes regulatory solutions.

A. Lack of Notice or Opt-Out Option

The mobility of MORIS does not give citizens notice of the device's use or the ability to opt out of getting scanned in the way stationary checkpoints allow. If using FRT is not a Fourth Amendment search, and probable cause or reasonable suspicion is not a prerequisite to data collection and use, then the police can legally take a picture of anyone and run it through the database without suspicion that the person has done something illegal.[146] Although people can opt out of going to sporting events or airports to avoid FRT and iris scans, people cannot opt out of going about their daily lives. Thus, no matter where one goes in the United States, the possibility exists that an officer may use MORIS to take a picture and run it through a database to learn that person's identity and criminal history. Because the device works from 5 feet away, this investigation could be done secretly. Just as covert GPS tracking can "alter the relationship between citizen and government in a way that is inimical to democratic society,"[147] covert FRT could similarly sabotage this relationship.

B. Discriminatory Targeting and Racial Bias Concerns

Moreover, unlike a stationary checkpoint, where all who pass by are subject to FRT, MORIS's portability grants police discretion in deciding whom to identify. Without guidelines, nothing prohibits police from acting on potential

146. *See supra* Parts II, III, IV.

147. *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)). "Awareness that the Government may be watching chills associational and expressive freedoms." *Id.*

racial, gender, or class biases.[148] Legally, law enforcement could primarily run pictures of a certain type of person, without justifiable cause. Jay Stanley, an ACLU senior policy analyst, worries about the new type of "facial profiling" MORIS could create.[149]

Not only may police take pictures discriminatorily, but a racial bias also may arise while police search for a match. MORIS finds the three most similar faces and displays these headshots on the screen; however, an officer makes the final selection as to which picture matches the person he is trying to identify.[150] If the police officer is of a different race than the person to be identified, the officer may not make this selection accurately.[151]

Psychology studies show that people can more accurately recall specific faces if they are of their own race rather than of another race.[152] Due to the "other-race effect," people outside one's own race subjectively look more alike[153] unless that person has had ample exposure to another race.[154] A Northwestern University study shows that the brain encodes same-race faces with an emphasis on unique identifiers; however, the brain does not encode other-race faces with this level of detail.[155] "Consequently, we have poorer memory for other-race faces, and are therefore *less likely to [recognize] them or to distinguish between them.*"[156]

Lay witnesses have made inaccurate lineup identifications because of the other-race effect.[157] In 1984, an innocent man was convicted of rape after the

---

148. However, MORIS offers some oversight of police because it does save a trail of the searches an officer makes with the device complete with a GPS component. Telephone Interview with Sean Mullin, *supra* note 1.

149. Tovia Smith, *New Police Scanners Raise 'Facial Profiling' Concerns*, NPR (Aug. 11, 2011, 9:58 PM), http://www.npr.org/2011/08/11/138769662/new-police-scanner-raises-facial-profiling-concerns. Amie Stepanovich, national security counsel for Electronic Privacy Information Center ("EPIC"), expresses concern that police may abuse the technology to target people in "specific religious clothing or attending controversial events." Parvaz, *supra* note 60.

150. BI2Technologies, *supra* note 56.

151. *See* Mo Costandi, *Why Do People of Other Races All Look Alike?*, GUARDIAN NEUROPHILOSOPHY BLOG (Aug. 15, 2011, 12:55), http://www.guardian.co.uk/science/neurophilosophy/2011/aug/15/people-other-races-look-alike.

152. *Id.*

153. *Id.*

154. Daniel B. Wright et al., *Inter-Racial Contact and the Own-Race Bias for Face Recognition in South Africa and England*, 17 APPLIED COGNITIVE PSYCHOL. 365, 365–71 (2003) (Black students, attending a university in South Africa and who had been exposed to Whites, could more accurately identify White faces in photographs than the White students in England without cross-race exposure could identify Black faces in photographs).

155. Heather D. Lucas et al., *Why Some Faces Won't be Remembered: Brain Potentials Illuminate Successful v. Unsuccessful Encoding for Same-Race and Other-Race Faces*, FRONTIERS HUM. NEUROSCIENCE, Mar. 8, 2011, at 1, 1–14.

156. Costandi, *supra* note 151 (emphasis added).

157. *See* Mark Roth, *Looking Across the Racial Divide: How Eyewitness Testimony Can Cause Problems*, PITT. POST-GAZETTE, Dec. 26, 2010, at A1.

victim, of another race, identified him as the perpetrator.[158] When the man was exonerated though DNA evidence, the victim said that the other-race effect contributed to her misidentification.[159] Given that MORIS creates a photographic lineup with the three most mathematically similar faces and that people struggle with distinguishing another race's facial features, the Arizona legislature should give police procedures to follow when making the final match.

The other-race bias can be reduced by informing the witness of the potential bias and by telling the witness to look for individual facial features instead of looking at the face as a whole.[160] In one study, researchers eliminated the other-race bias by giving these warnings before the brain could encode the face.[161] To ensure more accurate identifications, officers using MORIS should be required to learn about other-race bias and how to look for unique features on faces of other races.

C. A Potentially Unduly Suggestive Lineup and Unreliable Identification

MORIS seemingly creates a de facto lineup in the field where police must identify a person from three photographs returned after a database search. Therefore, the procedures police follow in true lineups should be analyzed to see if officers are taking necessary steps to ensure that MORIS's identifications are not unduly suggestive or unreliable. In particular, police should make MORIS identifications in compliance with the *Biggers* factors to facilitate reliable identifications.

When police conduct photographic lineups and allow witnesses to identify whom they saw commit a crime, the procedure must not be unduly suggestive.[162] If an identifying procedure draws attention to a lineup participant as if to say that person committed the crime, the resulting identification usually must be suppressed to avoid mistaken identification and a denial of due process.[163] In *Foster v. California*, for example, the police placed the key subject in a lineup, conducted a one-to-one confrontation, and led another lineup with only that suspect returning.[164] "The suggestive elements in this identification procedure made it all but inevitable that [the witness] would identify petitioner whether or not he was in fact 'the man.'"[165]

---

158. *Id.*

159. *Id.*

160. Kurt Hugenberg et al., *Categorization and Individuation in the Cross-Race Recognition Deficit: Toward a Solution to an Insidious Problem*, 43 J. EXPERIMENTAL SOC. PSYCHOL. 334, 340 (2007). Learning to spot and encode facial attributes belonging to specific individuals is called perceptual individuation. Lucas et al., *supra* note 155, at 1.

161. *Id.*

162. Stovall v. Denno, 388 U.S. 293, 302 (1967).

163. *See id.*

164. Foster v. California, 394 U.S. 440, 443 (1969).

165. *Id.*

Showing a single picture to a witness, or undercover officer, can be mildly, and not unduly, suggestive if displayed under mitigating circumstances.[166] For example, the court in *Manson v. Brathwaite* noted that there was "little urgency and [the officer] could view the photograph at his leisure. . . . The identification was made in circumstances allowing care and reflection."[167] Even though the undercover officer was only shown one photograph, the lineup was not unduly suggestive because the person making the identification had less pressure to agree with the photo because he had time to reflect.[168]

Regardless of suggestive lineup procedures, the trial court must admit pretrial identifications into evidence if they are reliable under the totality of the circumstances.[169] To determine reliability, the court employs the *Biggers* five-factor test.[170]

> [T]he factors to be considered in evaluating the likelihood of misidentification include the opportunity of the witness to view the criminal at the time of the crime, the witness' degree of attention, the accuracy of the witness' prior description of the criminal, the level of certainty demonstrated by the witness at the confrontation, and the length of time between the crime and the confrontation.[171]

Strong reliability in one factor may compensate for a weakness in another factor.[172] Where only one photo was shown to an officer to see if he could identify the suspect, the Court held this to be mildly suggestive, but it was still admissible because it was reliable.[173] It was reliable because (1) the officer saw the assailant for two to three minutes in natural light; (2) the officer was trained to pay attention to detail and be attentive; (3) the physical description initially provided matched the photograph; (4) the officer had 100% certainty that the man in the photo was the same as the one he witnessed commit the crime; and (5) the photographic identification was made two days later so as not to allow the officer to forget the suspect's appearance.[174]

After taking a picture of someone's face with MORIS and running it through the database, the officer gets three images that most closely match that face via mathematical algorithms.[175] Because the officer evaluates which photo best resembles the person whose photo was taken,[176] MORIS creates a photographic lineup where law enforcement steps into the shoes of a witness. For

---

166. Manson v. Brathwaite, 432 U.S. 98, 116 (1977).
167. *Id.*
168. *Id.*
169. Neil v. Biggers, 409 U.S. 188, 199 (1972).
170. *Id.* at 199–200.
171. *Id.*
172. *Id.* at 199.
173. *Manson*, 432 U.S. at 109, 115–16.
174. *Id.* at 114–16.
175. BI2Technologies, *supra* note 56.
176. *Id.*

accuracy, identifications made by officers via MORIS should be held to similar standards as identifications made by witnesses via lineups.

MORIS's current identification procedure may be unduly suggestive—an officer could be overly confident in his reliance on technology[177] and feel as though the person standing in front of him is definitely a match to one of the photographs MORIS displayed. Granted, MORIS does not return a single picture,[178] but it does return the three most mathematically similar pictures out of the hundreds analyzed.[179]

Because an officer only receives three pictures, there may be a problem with the officer using a "relative judgment process"[180] whereby the officer selects the photo that looks most similar to the person law enforcement is trying to identify, relative to the other options.[181] Even if the person to be identified is not among the photographs MORIS loads, "the relative judgment process will nevertheless yield a positive identification because there will always be someone who looks more like the culprit than do the remaining lineup members."[182] Police could potentially arrest an innocent person and unreasonably restrain his freedoms if they make an incorrect identification. However, if the officer compares each MORIS option directly with the original photo or with the person's facial appearance in real-time instead of comparing the options among each other, this "absolute judgment"[183] would reduce the unduly suggestive aspects of MORIS.

Given that the de facto photographic lineup occurs in the field, the officer may feel added pressure to quickly make a selection, which could lessen the identification's accuracy. Unlike in *Manson*, where the officer could analyze a photograph leisurely,[184] the use of MORIS in the field could hasten analysis; an officer may quickly select the most similar photo to see that person's criminal history to determine if there is a safety threat.

To determine if lineup identifications are reliable, and thus admissible, courts weigh all factors of the *Biggers* test. Admittedly, this Note's analysis does not concern introducing MORIS identifications into evidence.[185] Nonetheless, this

---

177. In the past, the legal community has quickly accepted other identification methods, such as bite-mark evidence, but experts now question their accuracy. Fernanda Santos, *Evidence from Bite Marks, It Turns Out, Is Not So Elementary*, N.Y. TIMES, Jan. 28, 2007, at WK4 ("A 1999 study by a member of the American Board of Forensic Odontology, a professional trade organization, found a 63 percent rate of false identifications.").

178. The Supreme Court has condemned single-suspect lineups as being unduly suggestive. Stovall v. Denno, 388 U.S. 293, 302 (1967).

179. BI2Technologies, *supra* note 56.

180. *See* Gary L. Wells et al., *Eyewitness Identification Procedures: Recommendations for Lineups and Photospreads*, 22 L. & HUM. BEHAV. 1, 10 (1998).

181. *Id.*

182. *Id.*

183. *Id.*

184. Manson v. Brathwaite, 432 U.S. 98, 116 (1977).

185. The proper analysis to determine whether FRT identifications are admissible probably involves the *Frye* standard or *Daubert* test. *See generally* John Nawara, Note,

Note considers the *Biggers* test and undue suggestiveness to analyze how identifications made through lineups are either reliable or unreliable. This is important because police using MORIS essentially engage in a photo lineup as the final step in identification.

An officer who obtains consent to take a picture and then runs it through the FRT database will likely get a good look at the subject's face and make a highly certain, immediate, and accurate identification. However, in certain circumstances, the officer's actions may not satisfy the *Biggers* factors. For instance, if a picture is taken under poor conditions, such as in a dimly lit area; if the officer has minimal opportunity to view the suspect; or if the officer is not particularly attentive to the subject or picture loaded into MORIS because of distracting events, then the identification may not be as reliable.[186]

A statute passed by the Arizona legislature should ensure that officer identifications with MORIS comport with the *Biggers* factors and are reliable. The pictures that load on MORIS should be big enough to give the officer ample opportunity to study the face and make a match. The officer should also minimize distractions and attentively study the pictures to choose a match. The statute should require a baseline percentage of certainty by the officer before selections.[187] The statute further requires MORIS-based identifications to be made by police officers; law enforcement should not be allowed to show the MORIS photographs to lay witnesses at the scene and ask which picture they think most resembles the suspect.

D. Context Bias

To avoid mistaken identification, police are encouraged to read instructional warnings to witnesses partaking in lineups so they know that the guilty party may not necessarily be shown and that it is not necessary to select anyone.[188] In one study, "[f]ailure to warn the eyewitness that the culprit might not be in the lineup resulted in 78% of the eyewitnesses attempting an identification from the culprit-absent lineup. This false identification rate dropped to 33% when the eyewitnesses were explicitly warned that the culprit might not be in the lineup."[189] Just as witnesses may feel pressure to select someone from a lineup, police officers may feel pressure to select a displayed picture. Police training should remind officers that the person they are trying to identify may not be among

---

Machine Learning: Face Recognition Technology Evidence in Criminal Trials, 49 U. LOUISVILLE L. REV. 601 (2011).

186. *See generally* Neil v. Biggers, 409 U.S. 188 (1972).

187. Although some officers may be willing to say they had the certainty level required by statute regardless of true certainty, articulating a statutory standard at least fleshes out expectations and could force police to explain the basis for their certainty.

188. *Eyewitness Identification*, INNOCENCE PROJECT, http://www.innocence project.org/fix/Eyewitness-Identification.php (last visited Mar. 1, 2013).

189. Wells et al., *supra* note 180, at 11.

the pictures MORIS retrieves.[190] The Arizona legislature should also require displaying this warning on the MORIS screen before the final selection.

The pressure on an officer to select someone from MORIS's options may be greater if the officer knows that the people in the database have criminal records[191] or if the officer just witnessed the suspect do something suspicious.[192] As a corollary example, when fingerprint examiners were told that the suspect supplying the fingerprints had confessed to the crime, one-third of the examiners falsely identified the suspect as matching the fingerprints they were analyzing.[193] Conversely, when these fingerprint examiners were not exposed to that particular bias, and looked at the fingerprints without a suggestive context, they did not give a false positive.[194] The context bias caused by making field identifications from a database of criminals after seeing someone do something suspicious could result in a false positive. While this context bias cannot be removed, as in the fingerprint example, perhaps if police undergo initial mandatory training where they learn about the potential to feel persuaded, they will be more cognizant of their selections.

E. Function Creep

Function creep arises when technology designed to be used in a specific way or for a distinctive purpose starts to be used in unanticipated ways or to serve unintended purposes.[195] A concern exists that the use of MORIS will shift from storing photographs of the guilty[196] to storing photographs of the innocent. This is problematic because people in prison or on probation have a reduced expectation of privacy.[197] The lower level of privacy afforded to prisoners and probationers comes from the state's special needs function to ensure safety. Conversely, innocent citizens retain protection from unreasonable, warrantless searches.

---

190. "The facial recognition module is not a positive identification tool, it's an investigatory tool." Telephone Interview with Sean Mullin, *supra* note 1.

191. Facial images currently in the database consist mostly of people who have been admitted to or released from correctional facilities. Steel & Angwin, *supra* note 2.

192. *See* Manson v. Brathwaite, 432 U.S. 98, 133 (1977) (Marshall, J., dissenting) (explaining that police heighten the chance for a witness to make an inaccurate identification when they reveal that they have additional evidence implicating the pictured person in the crime).

193. *See* Achraf Farraj, Note, *Refugees and the Biometric Future: The Impact of Biometrics on Refugees and Asylum Seekers*, 42 COLUM. HUM. RTS. L. REV. 891, 939 (2011).

194. *Id.*

195. *See* CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING AND EAVESDROPPING § 31:50 (2012), *available at* Westlaw WIRETAP.

196. Steel & Angwin, *supra* note 2.

197. *See* United States v. Knights, 534 U.S. 112, 113 (2001); Griggin v. Wisconsin, 483 U.S. 868, 873–74 (1987); State v. Montgomery, 566 P.2d 1329, 1330 (Ariz. 1977).

Currently, MORIS does not save the images run through the program,[198] but relying on a technical restraint to construct a safeguard is unworkable. BI2 Technologies, or a competing company, could choose to store these images. BI2 Technologies has already expressed interest in compiling data from other databases; it sees a benefit in including driver's license photos.[199] Similar programs, like the Automated License Plate Recognition system, store license plate numbers of the innocent and guilty so the database can be mined during Amber Alerts or for leads in cases.[200] If police know that the databases MORIS uses could be mined in other events, they may have an incentive to expand the databases by taking photographs of persons without any level of suspicion for wrongdoing. And although the Automated License Plate Recognition Program is legal, there is something inherently more private about our faces than our license plates.

"Our country has a long history of function creep—of databases, which are created for one discrete purpose and, which despite the initial promises of their creators, eventually take on new functions and purposes," said Barry Steinhardt, ACLU associate director in 2000.[201] For example, social security numbers that were originally to be used for retirement purposes, are now also used to identify individuals in a variety of settings.[202]

Many law enforcement agencies using MORIS have vowed to only use the technology in certain circumstances. The Pinellas County Sheriff's Office, in Florida, obtains consent before taking someone's picture.[203] The Brockton, Massachusetts, police department announced that it would only use MORIS when actively searching for someone or when someone has committed an offense.[204] Likewise, the Pinal County Sheriff's Office said it will only use FRT to identify "people suspected of arrestable offenses" or people from whom the officers have obtained consent.[205] However, these law enforcement agencies could choose to expand the use of FRT beyond what they have set forth as their limits.

Some police departments have already demonstrated a willingness to use stored pictures and information about license plates to follow gang members.[206]

---

198. Telephone Interview with Sean Mullin, *supra* note 1.

199. Steel & Angwin, *supra* note 2.

200. Hilary Hylton, *License-Plate Scanners: Fighting Crime or Invading Privacy?*, TIME (July 30, 2009), http://www.time.com/time/nation/article/0,8599,1913258,00.html.

201. *CODIS: Hearing on H.R. 3375 Before the Subcomm. on Crime of the H. Comm. on the Judiciary*, 106th Cong. 178 (2000) (statement of Barry Steinhardt, former Associate Director, ACLU), *available at* http://www.aclu.org/technology-and-liberty/testimony-barry-steinhardt-codis-house-judiciary-subcomitteee-crime.

202. *Id.*

203. Murray, *supra* note 21.

204. Clay Dillow, *iPhone Armed with Facial Recognition App Lets Cops ID Perps on the Street*, POPULAR SCI. (June 15, 2010, 10:30 AM), http://www.popsci.com/technology/article/2010-06/police-get-facial-recognition-iphone-app-id-perps-field.

205. Groff, *supra* note 15.

206. Hylton, *supra* note 200.

The Los Angeles Police Department wanted to use license plate information for more purposes but had to limit its use due to public pushback.[207] While it is a violation of Pinellas County Sheriff's Office's guidelines to learn the identity of people without consent, it would be acceptable under the Fourth Amendment.[208] Therefore, MORIS's use creates a potential for function creep.

F. Enrollment of Data and Database Security

To ensure the privacy of biometric information, MORIS users should have to comply with a data management plan that regulates who can access the data and how the database can expand.[209] Currently, MORIS accesses a criminal justice database of criminal records, iris scans, and face images contributed by local law enforcement that use products by BI2 Technologies.[210] Although some states have added mug shots, the database mainly consists of people who have been admitted or released from correctional facilities.[211] As designed, MORIS does not save a picture of a face[212] or iris[213] that goes through either the face or iris database. BI2 Technologies manages the databases[214] but will not sell the data because it does not own it.[215]

The Privacy Act of 1974[216] outlines how the federal government may collect, maintain, use, and disseminate personal information—including biometrics—of U.S. citizens and legal residents.[217] A federal agency with records containing personal identifiers must allow the individual to control information use and dissemination; let the individual correct or amend the information; create safeguards; and make known the records' existence through publication.[218] However, the Privacy Act does not apply to state and local governments,[219] so it would seemingly not be applicable to the iris and face databases that local and state law enforcement agencies contribute to and use with MORIS.

---

207. *Id.*
208. *See supra* Part IV.
209. *See* Smith, *supra* note 149.
210. Steel & Angwin, *supra* note 2.
211. *Id.*
212. Ebbert, *supra* note 31.
213. Smith, *supra* note 149.
214. Steel, *supra* note 13.
215. Steel & Angwin, *supra* note 2. The information is held in a type of public trust. Telephone Interview with Sean Mullin, *supra* note 1.
216. 5 U.S.C. § 552a (2012).
217. NAT'L BIOMETRIC SEC. PROJECT, UNITED STATES FEDERAL LAWS REGARDING PRIVACY AND PERSONAL DATA AND APPLICATIONS TO BIOMETRICS 40–42 (2006), *available at* http://danishbiometrics.files.wordpress.com/2009/08/usfederalprivacyreport0306.pdf.
218. *Id.*
219. *Id.*

The Arizona legislature should establish who can access the database[220] and when local and state agencies can share iris information, facial images, and criminal histories to ensure that the data is only used for law enforcement. For iris scans in particular, more information than just the person's identity is revealed: Iris scans can show diseases.[221] If iris information were not limited to use by law enforcement, but could be sold to private parties, this could be detrimental to the sick—especially in regard to insurance coverage and job offers.[222] Criminal records, which are subject to an enhanced privacy interest, also need protection.[223] Limiting who has access to this data is important because others can learn more about a person as datasets are matched and distributed. For example, in a Carnegie Mellon University study, researchers could predict social security numbers of subjects via FRT combined with the subjects' Facebook information.[224]

The Arizona legislature should prescribe when law enforcement can save facial pictures or iris scans.[225] A Privacy Policy Guidance Memorandum issued by the Department of Homeland Security ("DHS") suggests that DHS databases retaining personal identifying information should only collect the data necessary to fulfill the specified purposes.[226] Although state and local law enforcement agencies

---

220. Currently, MORIS has five levels of security, which includes authorizing an officer to a device; requiring network recognition of the device; and forbidding data to be saved on the handheld device. Telephone Interview with Sean Mullin, *supra* note 1.

221. Ridza Azri Ramlee et al., *Detecting Cholesterol Presence with Iris Recognition Algorithm*, *in* BIOMETRIC SYSTEMS, DESIGN AND APPLICATIONS 129, 146 (2011), *available at* http://cdn.intechopen.com/pdfs/21767/InTech-Detecting_cholesterol_presence_with_iris_recognition_algorithm.pdf (explaining that iris scans can reveal cholesterol in one's system); Patrick J. Morrison, *The Iris—A Window into the Genetics of Common and Rare Eye Diseases*, 79 ULSTER MED. J. 3, 3–5 (2010) (noting that some chromosome disorders like Down syndrome and Williams syndrome can be detected from iris patterns).

222. Eur. Parl. Ass., *supra* note 141, at 9.

223. U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 767 (1989).

224. Kashmir Hill, *How Facial Recognition Technology Can Be Used to Get Your Social Security Number*, FORBES (Aug. 1, 2011, 10:50 AM), http://www.forbes.com/sites/kashmirhill/2011/08/01/how-face-recognition-can-be-used-to-get-your-social-security-number/ (explaining how the dataset of anonymous faces could be matched with data on Facebook to learn these people's hometowns and birth years to then predict their social security numbers).

225. *See* David McCormack, Note, *Can Corporate America Secure Our Nation? An Analysis of the Indentix Framework for the Regulation and Use of Facial Recognition Technology*, 9 B.U. J. SCI. & TECH. L. 128, 152 (2003) (citing Quentin Burrows, Note, *Scowl Because You're on Candid Camera: Privacy and Video Surveillance*, 31 VAL. U. L. REV. 1079, 1112 (1997)).

226. Privacy Policy Guidance Memorandum from Hugo Teufel III, Chief Privacy Officer of the U.S. Dep't of Homeland Sec., on The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security 4 (Dec. 29, 2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

are not required to follow this direction from the Privacy Office for the DHS,[227] a similar approach could be taken here.

There is currently little guidance as to when and how facial pictures and iris scans should be stored; however, the challenge to mandatory DNA collection as a prerequisite to pretrial release in *United States v. Pool*[228] may shed light on collecting facial photos and iris scans of the unconvicted. In *Pool*, the federal government collected the DNA of a man who had not yet been convicted to be stored in the Combined DNA Index System ("CODIS"), which allows federal, state, and local law enforcement to search the database for matches from crime scenes.[229] Pool argued that the collection violated his Fourth Amendment rights, that the DNA revealed more about him than just his identity, and that there were inadequate assurances that the DNA would be used only for identification purposes.[230] A three-judge panel at the Ninth Circuit upheld the collection.[231] An en banc panel for the Ninth Circuit was scheduled to hear the case on September 20, 2011,[232] but Pool pled guilty, so the argument was dismissed as moot leaving no precedent.[233] Granted, this Note proposes that taking pictures of someone's face, running them through the database, and storing them does not implicate Fourth Amendment protections.[234] Nonetheless, storing iris information raises some of the same concerns Pool's case did because iris scans reveal health information in addition to identity, and this information could be misused.

VI. A LEGISLATIVE RESPONSE REQUIRED: SELF-REGULATION BY LAW ENFORCEMENT OR MORIS'S DEVELOPER IS UNWORKABLE

The Arizona legislature has taken the first step needed to regulate MORIS by recognizing that biometric identification technology needs constraints.[235] In 2008, the legislature prohibited public schools and charter schools from collecting students' biometric information—including fingerprints and the characteristics of eyes, hands, or the face—without parental consent.[236] This is a step in the right direction. The next step is outlining how Arizona law enforcement should use MORIS.

---

227. U.S. Dep't of Homeland Sec., *Privacy Policy Guidance*, U.S. DEPT. HOMELAND SEC., http://www.dhs.gov/files/publications/gc_1271701587683.shtm (last modified Jan. 30, 2012).

228. Electronic Privacy Info. Ctr., *U.S. v. Pool: Concerning the Constitutionality of Mandatory DNA Collection*, EPIC, http://epic.org/amicus/pool/ (last visited Mar. 4, 2013).

229. *Id.*

230. *Id.*

231. *Id.*

232. *Id.*

233. Shaun Martin, *U.S. v. Pool (9th Cir.- Sept. 19, 2011)*, CALIF. APP. REP. BLOG (Sept. 20, 2011, 10:39 AM), http://calapp.blogspot.com/2011/09/us-v-pool-9th-cir-sept-19-2011.html.

234. *See supra* Part IV.

235. *See* ARIZ. REV. STAT. ANN. § 15-109 (2013).

236. *Id.*

BI2 Technologies, MORIS's developer, cannot be expected to limit its designs to solve privacy and policy concerns or to develop rules for agencies buying its products. Unless companies designing FRT think a government's threat of regulation is credible, there may be little incentive to self-regulate.[237]

> We're the creators of technology. We don't decide public policy, we don't do legislation, we don't do regulation, we don't do policies and procedures. But, we build every single safeguard possible to ensure that the intended purpose of it is what it will actually accomplish in a safe, responsible manner that will protect everyone's constitutional rights and safety.[238]

BI2 Technologies has taken efforts to ensure that only personnel authorized on the network and the device can operate MORIS and that the data does not stay on the device.[239] However, nothing seems to prevent the company from altering the design's safeguards.[240] Furthermore, while the physical device may not retain data, MORIS may be capable of allowing its users to enroll a picture of the subject's face into the database.[241] No Arizona statutes address how to build the facial and iris databases.[242]

Law enforcement should not be left to self-regulate. While firms and industries sometimes self-regulate to the extent necessary to insulate their current use of technology from government regulation, such efforts are often insufficient to eliminate negative externalities.[243] Likewise, law enforcement acting alone will likely be unable to strike the proper balance between using MORIS to derive positive results and safeguarding citizens' privacy and policy concerns. Self-regulation is also troubling when guidelines fail to address a problem in its entirety; for example, if internal police guidelines only solve privacy and not

---

237. McCormack, *supra* note 225, at 145–47.

238. Telephone Interview with Sean Mullin, *supra* note 1.

239. *Smart Phone Face Scan Tech a Privacy Breach?*, CBSNEWS (July 15, 2011, 10:32 AM), http://www.cbsnews.com/stories/2011/07/15/earlyshow/leisure/gamesgadgets gizmos/main20079772.shtml (quoting Sean Mullin, President & CEO, BI2 Technologies). To use MORIS, officers must be pre-authenticated on both the network and device. *Id.*

240. *Id.* ("The fact that they're agreeing voluntarily not to retain information doesn't keep them from deciding at some point in the future that they will." (quoting John Reinstein, Legal Dir., ACLU of Mass.)).

241. Mullin says MORIS cannot enroll facial pictures into the database. Telephone Interview with Sean Mullin, *supra* note 1. *But see* Kieffer & Trissell, *supra* note 35 (showing that other handheld biometric devices, such as those used by the military, have enrollment capability); BI2 Technologies, *supra* note 56.

242. Westlaw search for "facial database," "iris database," and "biometric" in the Arizona Statutes Annotated database yielded no relevant results.

243. *See* Michael Lenox, *Do Voluntary Standards Work Among Corporations? The Experience of the Chemicals Industry*, *in* MAKING GLOBAL SELF-REGULATION EFFECTIVE IN DEVELOPING COUNTRIES 62, 64, 66 (Dana Brown & Ngaire Woods eds., 2007); *see also* Victor T. Nilsson, Note, *You're Not from Around Here, Are You? Fighting Deceptive Marketing in the Twenty-First Century*, 54 ARIZ. L. REV. 801, 813–15 (2012) (arguing that Google's efforts to self-police against deceptive search engine optimization are inadequate to prevent related harm to consumers and the marketplace).

policy concerns, then the concerns about racial bias and inaccurate identifications remain unaddressed. Also, if the public lacks the opportunity to comment on agency-made guidelines or to scrutinize these guidelines, then the public faces an uphill battle trying to hold law enforcement accountable. This Note next analyzes the internal MORIS guidelines law enforcement agencies have adopted to discover shortcomings and propose solutions.

A. Law Enforcement Agencies' Proposed Guidelines for MORIS

The Pinal County Sheriff's Office has told reporters several of its self-imposed restrictions for taking facial pictures and searching the database: Deputies can only verify the identification of someone who has been arrested or of someone who is not carrying an identification card.[244] For the iris scans, Sheriff Paul Babeu suggested that deputies first need to either have consent or probable cause.[245] No newspapers or magazines published in 2011 raised policy issues of officer error in regard to MORIS.[246] Thus, it is unclear if the Pinal County Sheriff's Office has procedures in place to combat the policy concerns raised in Part V of this Note.

Available journalism does, however, show the standards some law enforcement agencies are using before taking pictures of a person's face and using MORIS's FRT. Sheriff Joseph McDonald, Jr., of Plymouth County, Massachusetts, told *The Wall Street Journal* reporters that his deputies would only take facial pictures and run them through the database if they had reasonable suspicion.[247] Scott McCallum, a systems analyst for the Pinellas County Sheriff's Office in Florida, said that his office would require deputies to ask for consent before taking a photo with MORIS and using its FRT.[248]

Police assurances that they will not use MORIS to take pictures without consent do not address the real concern that these technologies may constitute Fourth Amendment searches. Hence, individuals subjected to such searches should receive the appropriate protections under the Fourth Amendment. Moreover, if the only guideline police agencies propose is to obtain consent before picture collection and analysis, then this does nothing to counteract possible police error and bias when the police officer selects one picture of the three MORIS suggests. Moreover, the guidelines are incomplete if they only address collecting a facial picture or iris scan and running these items through a database; guidelines must also address how and when data can be stored.

---

244. Steel & Angwin, *supra* note 2.

245. James Careless, *Latest Facial Recognition Solutions, The Eyes Have It*, GOV'T VIDEO (Sept. 28, 2011), http://www.governmentvideo.com/article/latest-facial-recognition-solutions-the-eyes-have-it/113214.

246. Google search for newspapers or magazines relating to MORIS.

247. Steel & Angwin, *supra* note 2. No other MORIS guidelines for Plymouth County were reported in 2011 magazines or newspapers. Google search for newspapers or magazines relating to MORIS.

248. Steel, *supra* note 13.

B. Recommended Guidelines and Safeguards for Law Enforcement Using MORIS

The Arizona legislature should adopt a statute that addresses the public's privacy and policy concerns for the collection, analysis, and storage of facial photos and iris scans via MORIS.

1. Privacy Concerns

Under the Fourth Amendment, law enforcement may take a picture of someone's face from a lawful vantage point without reasonable suspicion or probable cause; there is no reasonable expectation of privacy as to the face, which is constantly exposed to the public.[249] However, in order to run the photograph through the MORIS database to determine identity and criminal history, police should follow existing rules for when they are authorized to demand identification.[250] Where there is reasonable suspicion that someone has or is about to commit a crime, police may conduct a *Terry* stop and demand the person's name under Arizona's stop-and-identify statute.[251] If the person fails to comply, the police may make an arrest.[252] Here, running a picture through the MORIS database would seem justified because the public expects to be identified in these situations. Similarly, if a police officer stops a car under proper authority and asks to see the driver's license, running a picture through MORIS seems acceptable because police have been given the authority to discover someone's identity in this situation. If, however, an officer approaches a person on the street with no reasonable suspicion, the encounter must be consensual; the person can leave and refuse to tell the officer his name without repercussions.[253] Where persons can currently refuse to reveal their identities, MORIS should not be used covertly. But, if police obtain voluntary consent to run a picture through the database, this should be allowed, and police need not inform the person of his right to refuse the consensual search. This follows the logic of *Schneckloth v. Bustamonte*, where police were not required to tell people of their right to refuse a consensual search.[254]

Before police can scan someone's iris, they should either gain consent or at least have reasonable suspicion, just as is required for fingerprints—the technology's most similar comparison. The state legislature should set forth this

---

249. *See* United States v. Dionisio, 410 U.S. 1, 14 (1973).

250. *See* United States v. Diaz-Castaneda, 494 F.3d 1146, 1151 (9th Cir. 2009) (citing United States v. Ellison, 462 F.3d 557, 566–67 (6th Cir. 2006) (Moore, J., dissenting) (suggesting that although there is no reasonable expectation of privacy in license plate numbers, a heightened suspicion may be needed for police to access more information about the driver or vehicle)).

251. ARIZ. REV. STAT. ANN. § 13-2412 (2013).

252. Hiibel v. Sixth Jud. Dist. Ct. of Nev., 542 U.S. 177, 186–90 (2004).

253. *See* Florida v. Royer, 460 U.S. 491, 497–98 (1983) (explaining that a person can decline to listen or respond to any question a police officer asks in a consensual encounter).

254. 412 U.S. 218, 231–32 (1973).

explicit requirement. The legislature should also mandate consent, or a minimum of reasonable suspicion that the person has committed a crime or is about to commit a crime, in order to run an individual's iris scan through the database.

2. Policy Concerns

There are several steps the Arizona legislature should take to minimize policy concerns arising from police using MORIS. First, to reduce the chance of officers displaying racial bias, the legislature should mandate law enforcement education about "other-race bias" and how to look for unique facial features of other races. At least one study shows that being warned of "cross-race effect" reduces this chance of bias.[255] Second, to minimize the risk of officers exhibiting the "relative judgment process," officers should be taught to compare each photo MORIS suggests directly with the subject's face or photograph. A warning that the subject may not be in the database should also appear on the MORIS screen. Third, police should learn about context bias to reduce false-positives. Fourth, the *Biggers* factors should guide officers making final identifications after MORIS retrieves possible matches. Officers should obtain clear pictures of subjects, minimize distractions, and dedicate a reasonable amount of time to studying the subject's face before making a selection. To unlock a photograph's attached criminal history, officers should be required to enter a certainty percentage regarding their selection to inhibit arbitrary identifications.

The Arizona legislature should also develop an appeals process for people to contest identifications made via MORIS. Technology and databases are imperfect; in one instance, a woman's social security number was accidently attached to another person's criminal record, which caused police—thinking there was a warrant for her arrest—to pull her over.[256] Police should inform citizens when they have been entered into a database, and they should be able to access the information to ensure its correctness; after all, people cannot appeal something about which they lack knowledge.

The legislature should specify the databases' purpose and who can access them to prevent function creep. Although BI2 Technologies does not own the databases MORIS uses, regulation should ensure that these databases stay publicly owned. Private database ownership raises concerns about selling personal data; for example, worries exist about private cellphone companies collecting personal information, such as customers' location data and Internet history, and selling it in anonymous form to third parties.[257] If the legislature does not adopt regulation to prevent private database ownership, there should at least be limits on a private company's ability to sell the data. BI2 Technologies, which has expressed an

---

255. Hugenberg et al., *supra* note 160, at 340.

256. Craig Thomas, *Bad Warrants: Mistaken Identity Leads*, TOLEDONEWSNOW.COM (Nov. 3, 2011, 8:15 PM), http://www.wtol.com/story/15956255/bad-warrants-mistaken-identity-leads.

257. David Goldman, *Your Phone Company Is Selling Your Personal Data*, CNNMONEY (Nov. 1, 2011, 10:14 AM), http://money.cnn.com/2011/11/01/technology/verizon_att_sprint_tmobile_privacy/index.htm.

interest in "building applications for the health-care and financial industries,"[258] could stand to profit if it owned biometric data and could sell database access to non-law enforcement agencies.

Also, the legislature should develop a process for enrolling an individual's information into the facial and iris databases. As discussed, the Fourth Amendment does not prevent police from taking a picture of anyone from a lawful vantage point,[259] so probably no further justification is needed to enroll pictures of the innocent, people engaged in suspicious behavior, or convicts. However, people engaged in suspicious behavior who are stopped by the police and are not already in the database may not have adequate incentive to be forthright about their identities. Before enrollment, precautions—beyond technology limitations—need to be in place to ensure information authenticity. The legislature should outline other forms of identification, such as a driver's license, that police should cross-check the individual's identity against before enrollment; relying on a person's word as to his identity is not sufficient. Consent for enrollment will not protect the database from people lying about their identities.

CONCLUSION

The Pinal County Sheriff's Office is among the 50 law enforcement agencies in the United States using MORIS without anything more than internal oversight and the technology's own restraints.[260] The Arizona legislature should set clear regulations for law enforcement's collection, use, and enrollment of facial information and iris scans. The public's privacy and policy concerns should inform the legislature's action. As Justice Alito writes in his concurring opinion for *Jones*, "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[261] Legislative action setting forth how law enforcement should use MORIS would proactively protect privacy instead of waiting for courts to interpret the minimal protections. Moreover, legislation would address policy concerns that would loom even if FRT and iris scans were Fourth Amendment searches. Ultimately, the benefits of MORIS must be tempered with respect for privacy and accuracy.

---

258. Steel & Angwin, *supra* note 2.

259. This is with the caveat that if the Supreme Court adopts the new mosaic theory, pervasive FRT from even a lawful vantage point may be a Fourth Amendment search. *See generally* United States v. Jones, 132 S. Ct. 945 (2012).

260. *See* Telephone Interview with Sean Mullin, *supra* note 1.

261. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring) (citation omitted).

***